



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/849,093	05/04/2001	Pracrit Garg	MSFT-0222/158379.2	9404
41505	7590	07/20/2006	EXAMINER DINH, MINH	
WOODCOCK WASHBURN LLP (MICROSOFT CORPORATION) ONE LIBERTY PLACE - 46TH FLOOR PHILADELPHIA, PA 19103			ART UNIT 2132	
PAPER NUMBER				

DATE MAILED: 07/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/849,093	Applicant(s) GARG ET AL.	
	Examiner Minh Dinh	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 May 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-10 and 12-32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-10 and 12-32 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 04 May 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. This action is in response to the RCE filed 05/10/2006.

Response to Arguments

2. Applicant's arguments filed 05/10/2006 have been fully considered but they are not persuasive. With respect to the rejections of claims 30-32 under 35 USC 101, Applicant argues that the claimed data structures is far more than the mere arrangement of information, but rather such data structures enable applications to rely on standard APIs and a standard data structure for implementing dynamic authorization policy (page 8, 2nd paragraph). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. Claims 30-32 do not recite either how the claimed data elements of the data structures enable applications to implement dynamic authorization policy or how the claimed data elements functionally/logically relate to each other so that the data structures as a whole can support specific functions when employed as a computer component.

With respect to the prior art rejections, Applicant argues that Swift remains an example of a system that enforces static access policy because the restricted token is evaluated the same way (page 9, 2nd paragraph).

Swift discloses that the restricted token is evaluated differently when there is a match for a security IDs in an access control entry (ACE) depending on whether the ACE is an allow ACE or a deny ACE (figures 6-7; col. 11, lines 21-56).

Applicant argues that Swift implicates static data because the restricted token includes no dynamic data to be evaluated at run-time. An access/unrestricted token associated with a user is static data because the same access token is generated each time the user logs on to the system (col. 4, lines 46-60). However, a restricted token is dynamic data because different restricted tokens will be generated for the same user according to dynamic factors such as different types of operations and/or applications (col. 7, lines 5-61). The restricted token is evaluated at run-time.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 30-32 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Regarding claim 30, it is directed to a data structure comprising an identifier for identifying the data structure and authorization policy data, which both are data. The claim

does not recite either how the claimed data elements of the data structure enable applications to implement dynamic authorization policy or how the claimed data elements functionally/logically relate to each other so that the data structure as a whole can support specific functions when employed as a computer component. Therefore, the claimed subject matter is nonfunctional descriptive material and is non-statutory.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 10 and 12-32 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Regarding claim 10, the limitation "tangible" (line 1) added to the claim according to the amendment filed 09/30/2005 was not disclosed in the originally filed specification and is considered new matter. It is suggested that Applicant replace the subject

matter "a tangible computer readable medium" with "a computer storage medium" (Specification, page 7, lines 14-23). Claims 12-32 are rejected on the same basis as claim 10.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-10 and 12-32 are rejected under 35 U.S.C. 102(e) as being anticipated by Swift (6,308,274).

The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was

derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

Regarding claims 1, 3-4, 10-15 and 22, Swift discloses a method for dynamically managing access to a resource in a computer system having a client making a request for the resource, the method comprising:

- computing a client authorization context after the request for the resource is received from the client (col. 4, lines 46-55);

- determining, via an application programming interface, based upon dynamic data and first dynamic policy whether the client authorization context is to be updated, wherein said first dynamic policy is tailored to an application through which the resource is accessed (col. 6, line 5 – col. 7, line 35);

- updating the client authorization context according to said determination (col. 6, line 5 – col. 7, line 35);

- comparing the client authorization context to at least one access control entry of an access control list (col. 7, lines 51-61);

- identifying an access control entry as an access control entry of type allow and when the allow access control entry applies in access evaluation, dynamic access check using dynamic data is automatically invoked (col. 5, lines 2-11; col. 7, lines 51-61; col. 11, lines 21-65), the

allow access control entry being functionally equivalent to a callback access control entry; and

in response to identifying the access control entry as a callback access control entry, evaluating, via said application programming interface, based upon the dynamic data and the second dynamic policy whether said allow access control entry bears on said access request, wherein said second dynamic policy is tailored to said application (col. 5, lines 2-11; col. 7, lines 51-61; col. 11, lines 21-65).

Regarding claim 2, Swift further discloses that the first dynamic policy defines flexible rules for determining the client authorization context (col. 6, lines 5-27; col. 12, lines) and wherein said second dynamic policy defines flexible rules for purposes of determining access privileges (col. 7, lines 51-61; col. 11, lines 21-65).

Regarding claims 5, 16 and 23, Swift further discloses that the evaluating based upon dynamic data includes invoking an application-defined dynamic access check routine that performs based in part upon dynamic data such as a Boolean expression in the access control list, the Boolean expression indicating a condition for granting access to the resource (col. 11, lines 21-65; col. 12, lines 46-67). Since access is evaluated using data in each access control entry, inherently, the Boolean expression is part of the callback access control entry.

Regarding claims 6, 17 and 24, Swift further discloses that the access check routine is invoked automatically when there is a match between an identifier in the client authorization context and an identifier in the callback access control entry (col. 7, lines 51-61; col. 11, lines 21-65).

Regarding claims 7 and 18, Swift further discloses registering with the operating system, which is the resource manager of the computer system, an application-defined routine for determining dynamic groups (col. 6, lines 38-47; col. 12, lines 36-67).

Regarding claims 8 and 19, Swift further discloses an application-defined routine for determining dynamic access checks is performed by the security mechanism in the kernel (col. 11, lines 10-20). Inherently, the routine is registered with the operating system, which is the resource manager of the computer system.

Regarding claims 9, 21 and 25, Swift further discloses that the evaluating based upon dynamic data and second dynamic policy supplements a determination of access rights based upon static data and policy (col. 11, lines 38-56).

Regarding claim 20, Swift further discloses comparing data to a client authorization context determined based upon static data and policy before determining whether the client authorization context is to be updated (col. 7, lines 5-22; col. 8, lines 8-17).

Regarding claim 26, Swift discloses for an application in a computer system having a resource manager that manages and controls access to a resource, carrying out a dynamic authorization callback mechanism that provides extensible support for application-defined business rules via a set of APIs and DACLS including a dynamic groups element, which enables an application to assign temporary group membership, based on dynamic factors, to a client for the purpose of checking access rights (col. 5, lines 2-28; col. 6, lines 15-27; col. 7, lines 5-22; col. 8, lines 30-60; col. 11, lines 10-56).

Regarding claim 27, Swift further discloses a dynamic access check element, which enables an application to perform dynamic access checks, via DACLS and APIs, said dynamic access checks being customized to the application (col. 13, lines 20-56).

Regarding claim 28, Swift further discloses that the dynamic groups element and a dynamic access element are performed at the operating system level (col. 13, lines 20-56). Inherently the elements are registered with the operating system which is the resource manager of the computer system.

Regarding claim 29, Swift further discloses that the dynamic groups element and a dynamic access element utilize dynamic data related to client operation (col. 12, lines 46-59; col. 13, lines 20-43).

Regarding claim 30, Swift discloses a data structure stored on a computer storage medium for use in connection with dynamic access check determinations for an application in a computer system, the data structure comprising: an identifier for identifying the data structure as an **allow** access control entry (col. 5, lines 2-11). Swift discloses that when a **deny** access control entry applies, no further testing is necessary but when an **allow** access control entry applies, dynamic access check using dynamic data is automatically invoked (col. 5, lines 2-11; col. 7, lines 51-61; col. 11, lines 21-65); therefore, the **allow** access control entry meets the limitation of a callback access control entry.

Swift discloses storing in an access control list dynamic authorization policy data in a format tailored to the application to handle access request (col. 11, lines 47-56; col. 12, lines 36-67). Since the dynamic authorization policy data indicates an allowable condition, inherently, it is part of the allow access control entry.

Regarding claim 31, Swift further discloses that the data structure comprises a security identifier for an access privilege check (fig. 5, element 80; col. 5, lines 2-11).

Regarding claim 32, Swift further discloses that the data structure comprises a list of access permissions for allowing access to a resource (fig. 5, element 80; col. 5, lines 2-11).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

IBM, "Securing and Managing Web Resources with IBM SecureWay Policy Director – White Paper"

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

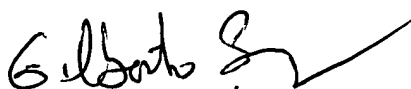
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MD

Minh Dinh
Examiner
Art Unit 2132

MD
7/13/06


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100